



IBM Security Verify の プロダクト・ツアー

ツアーを開始 →



あらゆるユーザーとあらゆるものを安全に接続

IBM Security Verify は、誰が何にアクセスすべきかという意思決定にコンテキストとインテリジェンスをもたらし、組織が適切な人に適切なタイミングでアクセス権を与えることを可能にします。

このデモを通してセキュリティーとユーザー・エクスペリエンスのバランスをマスターする方法を探りましょう。



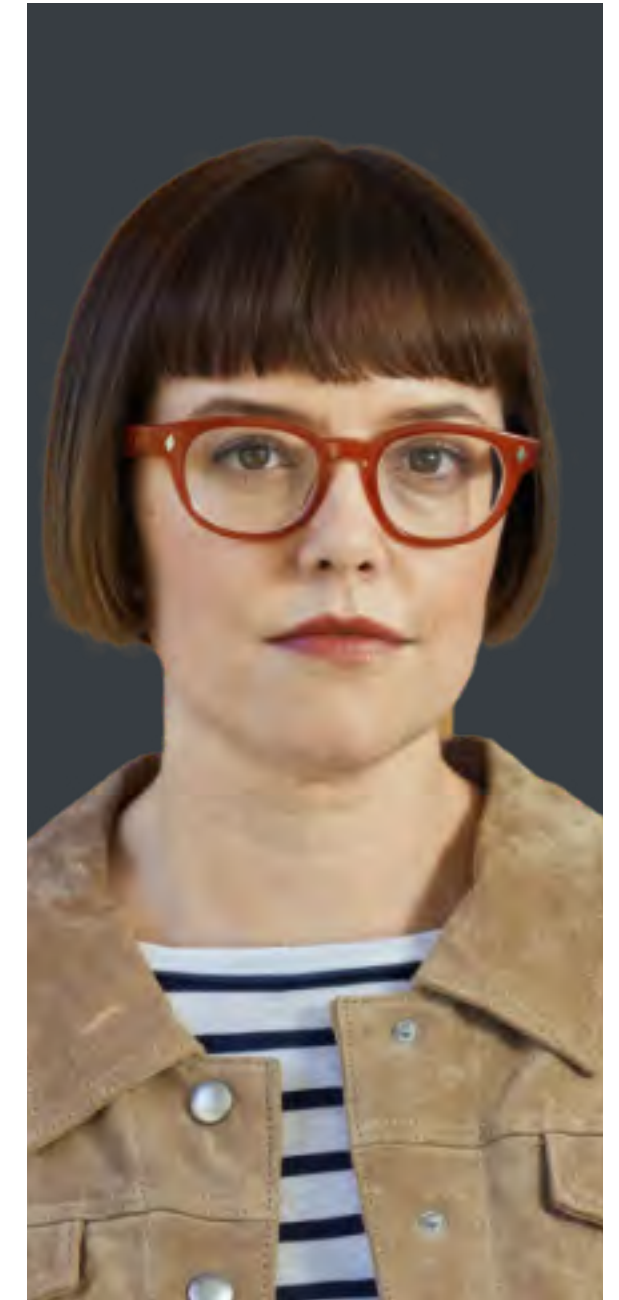
従業員



ビジネス管理職



IT 管理者



開発者




従業員

どのデバイスからでも、パスワードに煩わされ
ることなく、業務に必要なアプリケーションに
簡単にアクセスできます。

従業員は、数十もの認証情報に煩わされるこ
となく、業務に必要なツールに素早くアクセス
する必要があります。企業にはセキュリティー
が期待される一方で、IT ポリシーが障害に感
じられることもあります。従業員は、障害物な
く効率的に働きたいと考えています。

次を開始：
ブランド化された
サインイン・ページ



11
時間
従業員がパスワードの入力や
再設定に費やす年間平均時間
世界経済フォーラム
「ただ仕事をしようとしているだ
けなのに、ツールやシステムに
阻まれるのは、本当に苦痛です。」
Jessica、従業員


従業員



表示



表示



表示



従業員



シングル・
サインオン



アプリケーション
へのアクセスを
要求



MFA を登録して
使用する



ビジネス管理職



IT 管理者



開発者




戻る

次へ

従業員

どのデバイスからでも、パスワードに煩わされ
ることなく、業務に必要なアプリケーションに
簡単にアクセスできます。

従業員は、数十もの認証情報に煩わされるこ
となく、業務に必要なツールに素早くアクセス
する必要があります。企業にはセキュリティー
が期待される一方で、IT ポリシーが障害に感
じられることもあります。従業員は、障害物な
く効率的に働きたいと考えています。



11
時間
従業員がパスワードの入力や
再設定に費やす年間平均時間
世界経済フォーラム
「ただ仕事をしようとしているだ
けなのに、ツールやシステムに
阻まれるのは、本当に苦痛です。」
Jessica、従業員

従業員

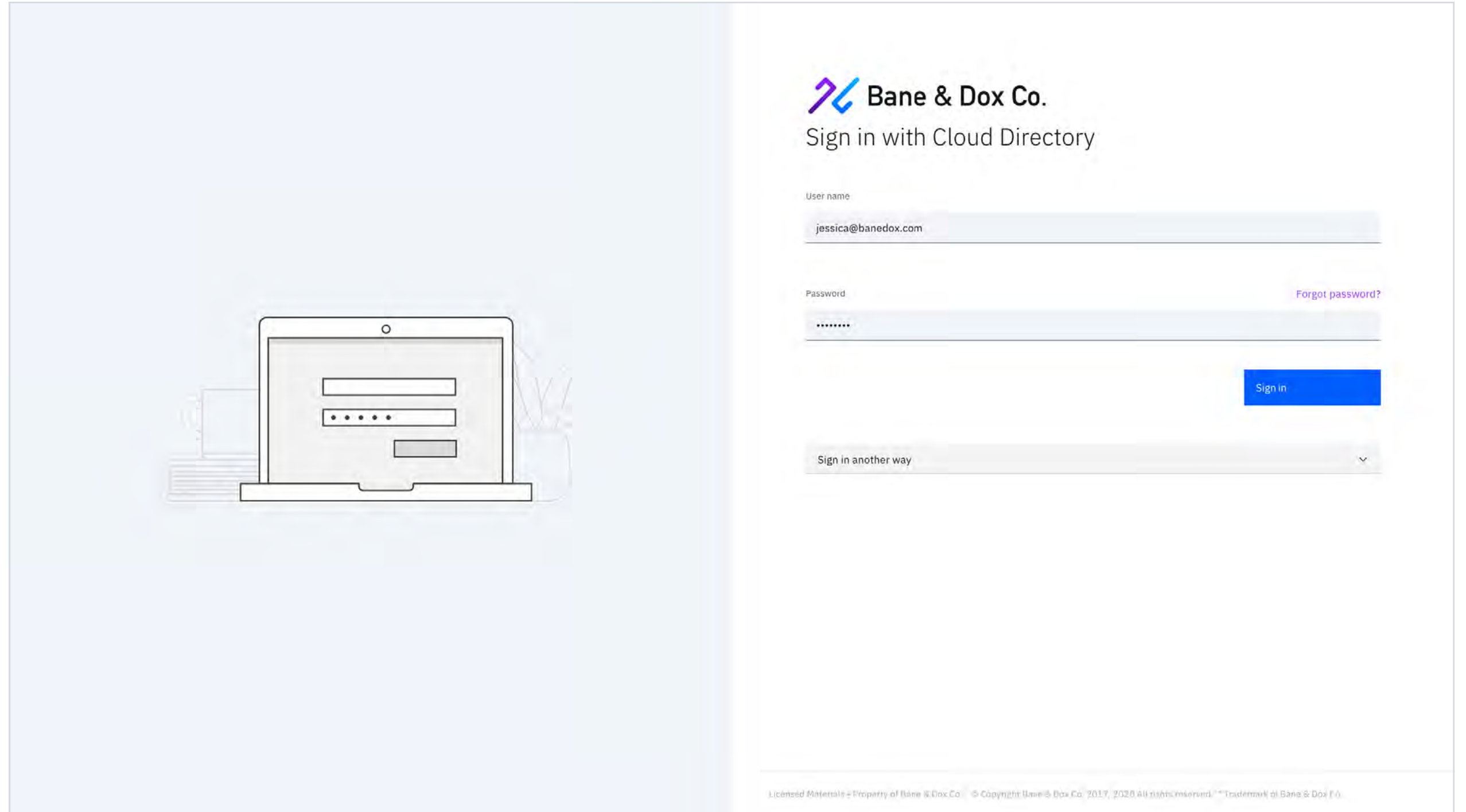
- 従業員
 - シングル・サインオン
 - ブランド化されたサインイン・ページ
 - ワンクリックでアプリにアクセス
 - アプリケーションへのアクセスを要求
 - カタログの検索
 - 正当性の根拠を書く
 - 処理待ちの要求
 - ランチパッドの新規アプリ
 - MFA を登録して使用する
 - 新規認証デバイスの追加
 - モバイルアプリの設定
 - MFA メソッドを選択
- ビジネス管理職
- IT 管理者
- 開発者

従業員: 1 / 2
シングル・サインオン

ブランド化された サインイン・ページ

従業員は、数十もの認証情報に煩わされることなく、業務に必要なツールに素早くアクセスする必要があります。企業にはセキュリティーが期待される一方で、IT ポリシーが障害に感じられることもあります。従業員は、障害物なく効率的に働きたいと考えています。

次は:
ワンクリックでアプリにアクセス



従業員



シングル・
サインオン



アプリケーション
へのアクセスを
要求



MFA を登録して
使用する



ビジネス管理職



IT 管理者



開発者



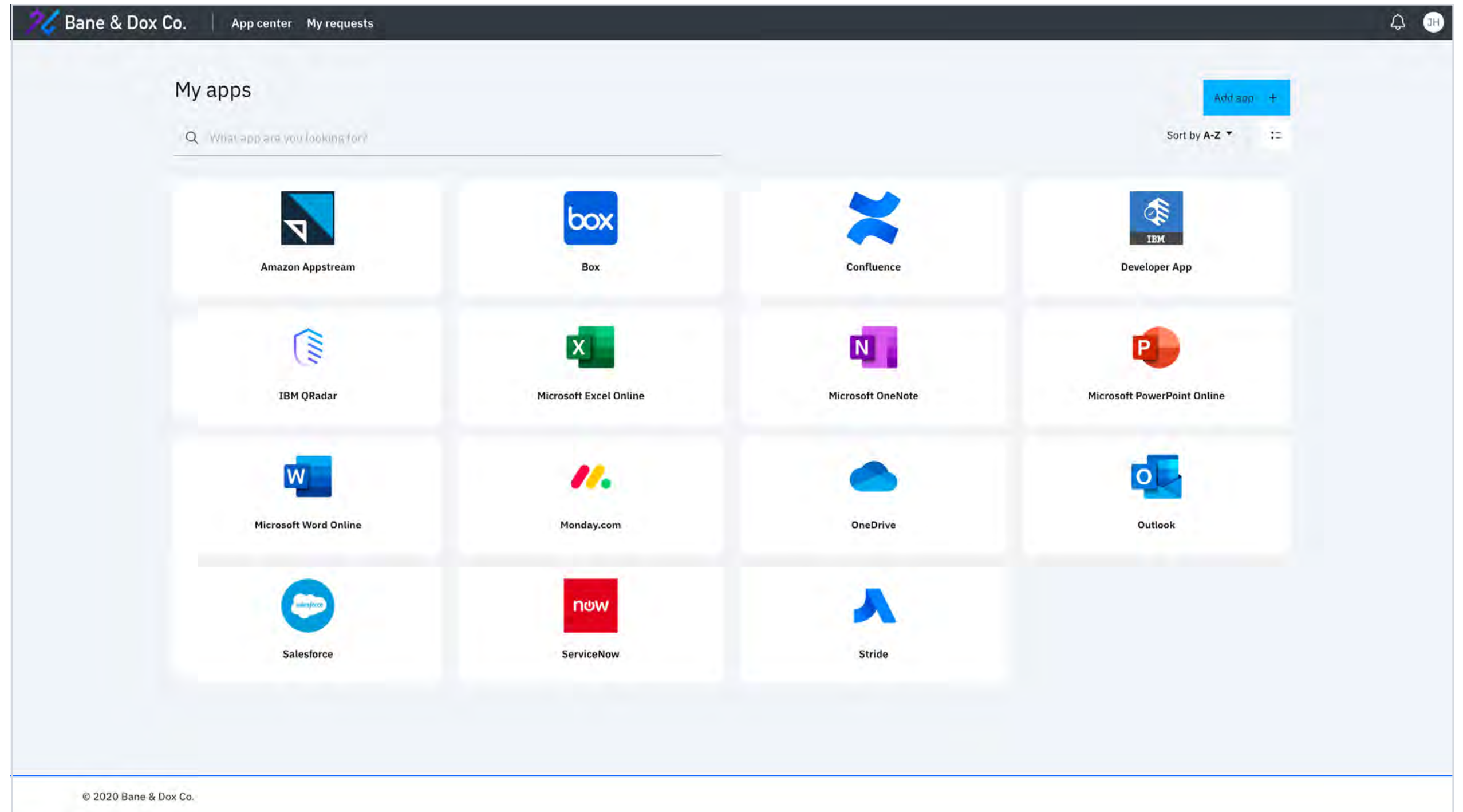
戻る

次へ

従業員: 2 / 2
シングル・サインオン

ワンクリックで アプリにアクセス

Jessica は自分のランチパッドから、利用権限があるすべてのアプリケーションにアクセスできます。IT 管理者がどのように設定するかにもよりますが、ほとんどのアプリケーションはワンクリックでアクセスできるようになっています。



次は:
カタログの検索



従業員

シングル・
サインオン

アプリケーション
へのアクセスを
要求

MFA を登録して
使用する

ビジネス管理職

IT 管理者

開発者



戻る

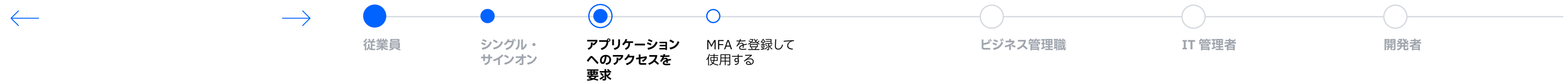
次へ

従業員: 1 / 4
 アプリケーションへのアクセスを要求

カタログの検索

Jessica は自分のランチパッドから、利用権限があるすべてのアプリケーションにアクセスできます。IT 管理者がどのように設定するかにもよりますが、ほとんどのアプリケーションはワンクリックでアクセスできるようになっています。

次は:
 正当性の根拠を書く



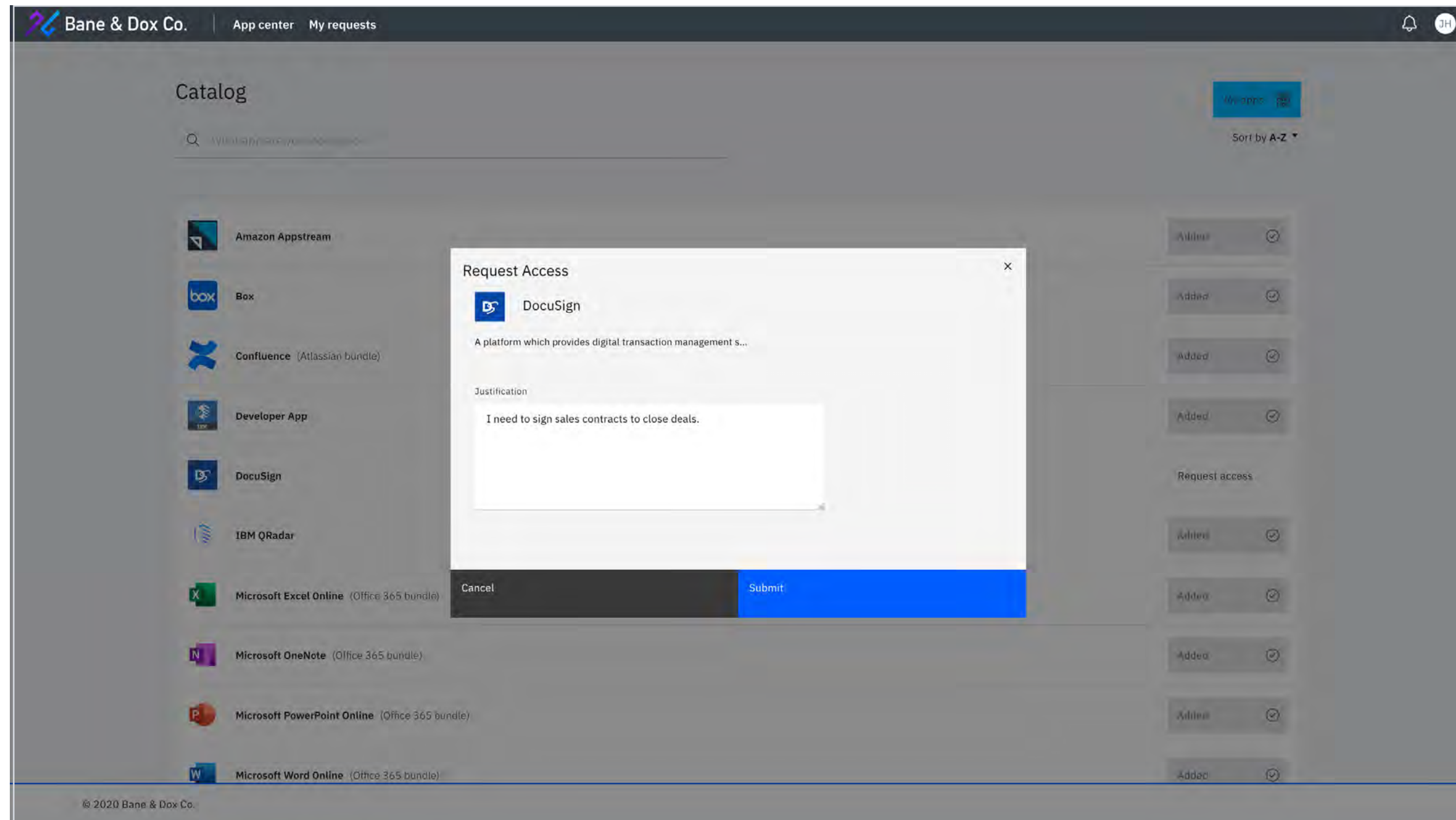
従業員: 2 / 4

アプリケーションへのアクセスを要求

正当性の根拠を書く

Jessica は XYZ を選択し、アクセス権が必要な理由について正当な事業上の根拠を書きます。

次は:
処理待ちの要求



従業員



シングル・サインオン



アプリケーションへのアクセスを要求



MFA を登録して使用する



ビジネス管理職



IT 管理者



開発者



戻る

次へ

従業員: 3 / 4

アプリケーションへのアクセスを要求

処理待ちの要求

処理待ちの要求のページでは、処理待ちのアクセス権の要求とその割り当て先、現在のステータスを確認できます。必要であれば、ここに戻って正当性の根拠を追加することもできます。

次は:
ランチパッドの新規アプリ



従業員



シングル・サインオン



アプリケーションへのアクセスを要求



MFA を登録して使用する



ビジネス管理職



IT 管理者



開発者

My Requests

Search: Pending

Name	Approver	Status	Request date
<input type="checkbox"/> DocuSign	Application owner	Pending	15th May 2020

Items per page: 50 | 1-1 of 1 items | 1 of 1 pages

© 2020 Bane & Dox Co.

従業員: 4 / 4
アプリケーションへのアクセスを要求

ランチパッドの 新規アプリ

その要求に対して、アプリケーション・オーナーから承認を受けると、Jessica のランチパッド上に XYZ が追加されます。

次は:
新規認証デバイス、
ランチパッドの追加

My apps

What apps are you looking for?

Sort by A-Z

© 2020 Bane & Dox Co.



従業員



シングル・
サインオン



アプリケーション
へのアクセスを
要求



MFA を登録して
使用する



ビジネス管理職



IT 管理者



開発者



戻る

次へ

従業員: 1 / 3

MFA を登録して使用する

新規認証デバイス、ランチパッドの追加

Jessica は、セキュリティー設定ページで、認証チャレンジに使用するデバイスとリソースを追加できます。IBM Security Verify モバイル・アプリで使用するために携帯電話を登録し、MFA(多要素認証)チャレンジを完了させるか、他の利用可能な方法を選択できます。

次は:
MFA の登録



従業員



シングル・サインオン



アプリケーションへのアクセスを要求



MFA を登録して使用する



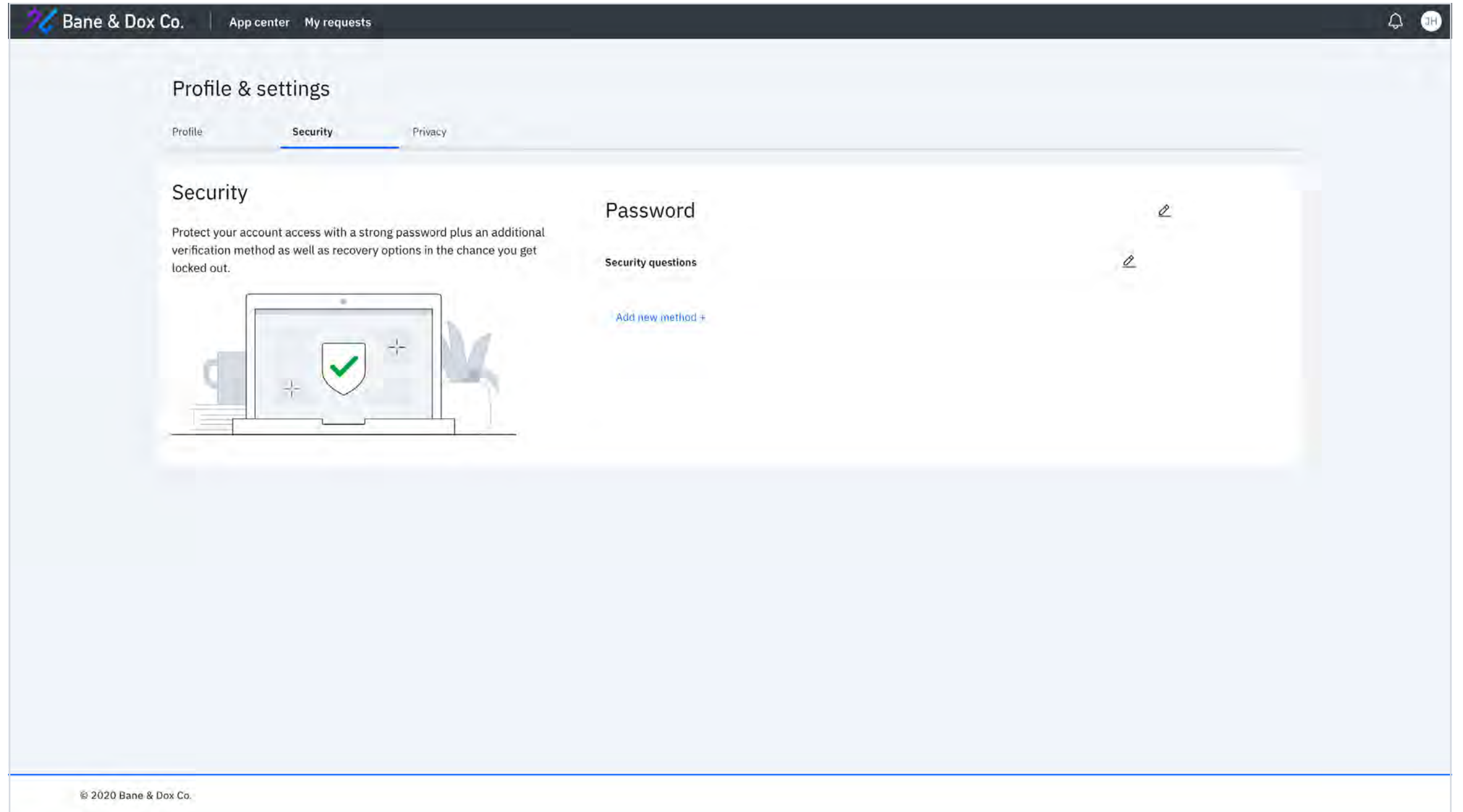
ビジネス管理職



IT 管理者



開発者

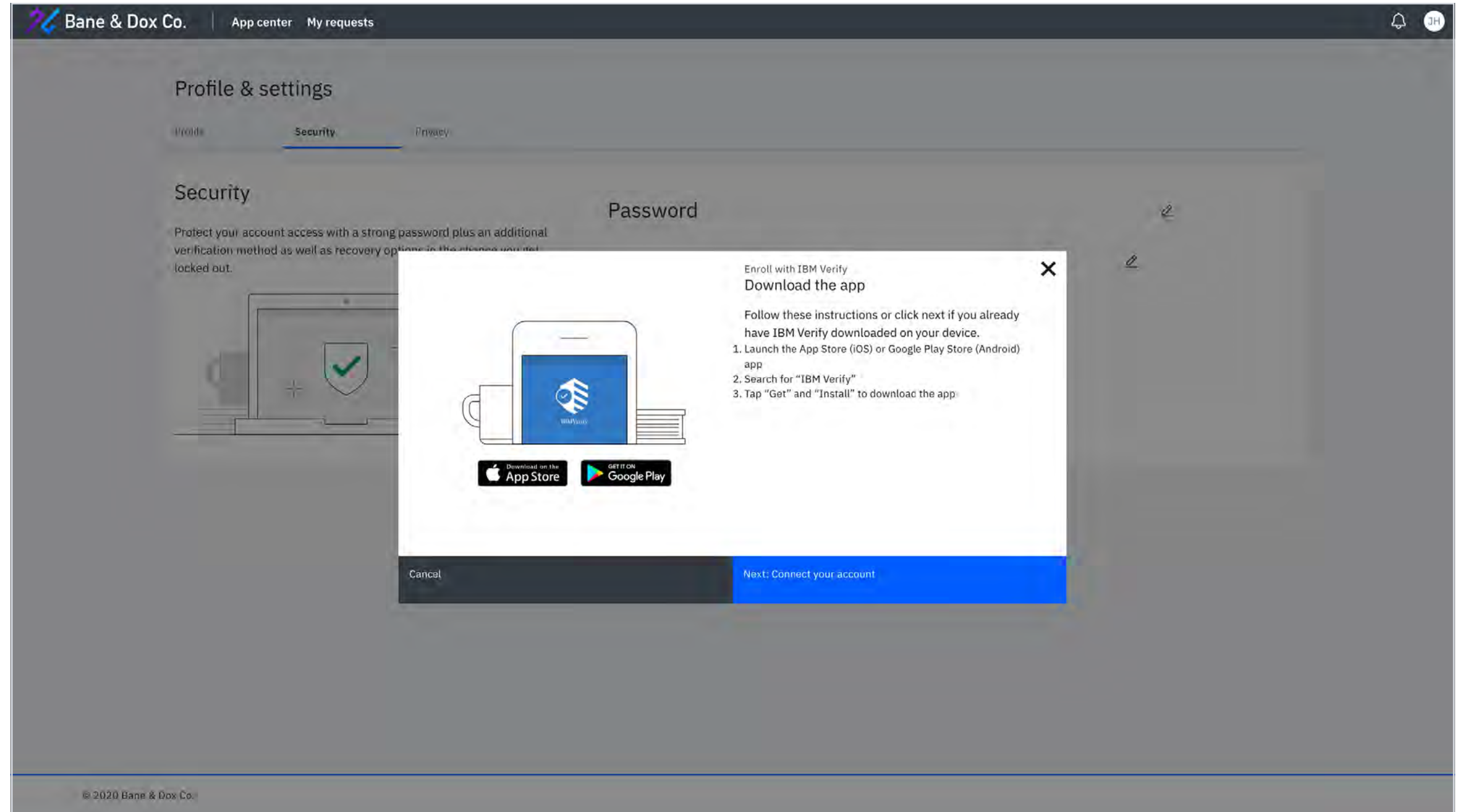


従業員: 2 / 3

MFA を登録して使用する

モバイルアプリの設定

Jessica は、セキュリティー設定ページで、認証チャレンジに使用するデバイスとリソースを追加できます。IBM Security Verify モバイル・アプリで使用するために携帯電話を登録し、MFA(多要素認証)チャレンジを完了させるか、他の利用可能な方法を選択できます。



次は:
MFA メソッドを選択



従業員

シングル・サインオン

アプリケーションへのアクセスを要求

MFA を登録して使用する

ビジネス管理職

IT 管理者

開発者



戻る

次へ

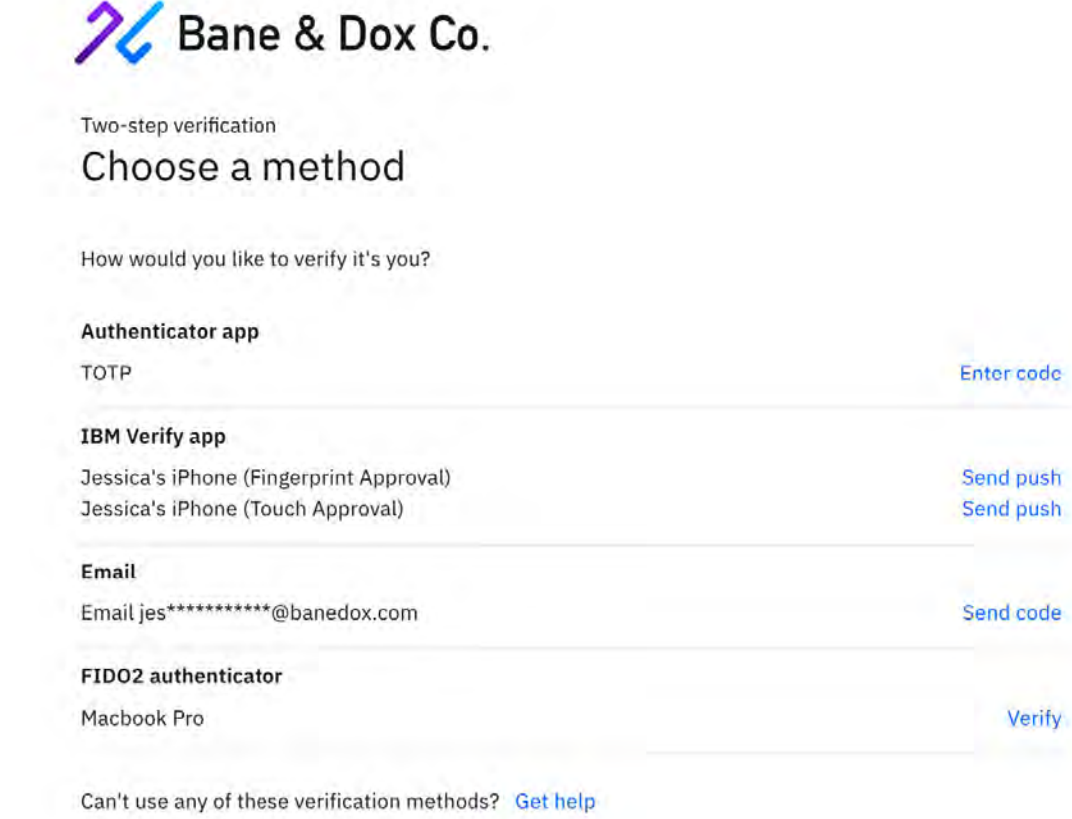
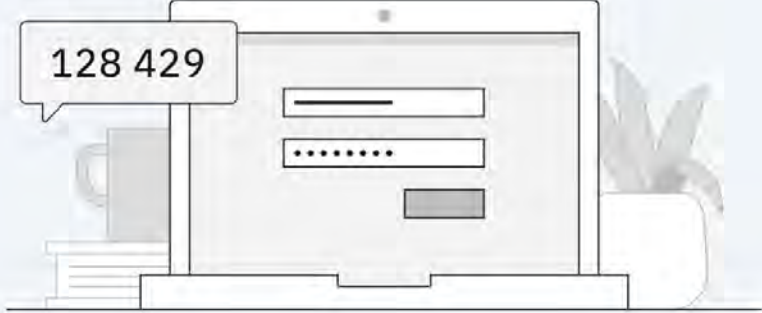
従業員: 3 / 3

MFA を登録して使用する

MFA メソッドを選択

これで、Jessica は MFA(多要素認証)を必要とするアプリケーションにログインする際、対応する認証方法の中から最も便利な方法を選択できるようになりました。

次は:
基幹業務の管理職



Two-step verification
Choose a method

How would you like to verify it's you?

Authenticator app
TOTP [Enter code](#)

IBM Verify app
Jessica's iPhone (Fingerprint Approval) [Send push](#)
Jessica's iPhone (Touch Approval) [Send push](#)

Email
Email jes*****@banedox.com [Send code](#)

FIDO2 authenticator
Macbook Pro [Verify](#)

Can't use any of these verification methods? [Get help](#)

Licensed Materials - Property of Bane & Dox Co. © Copyright Bane & Dox Co. 2017, 2020. All rights reserved.™ Trademark of Bane & Dox Co.



従業員



シングル・サインオン



アプリケーションへのアクセスを要求



MFA を登録して使用する



ビジネス管理職



IT 管理者



開発者



戻る

次へ

基幹業務の管理職

委任されたコントロールで、チーム固有のアプリケーションの権限付与を管理します。

基幹業務の管理職は、競争力を維持するために、新規サービスを従業員やお客様に迅速に提供する必要があります。IT の対応を待つことなく、ビジネスのスピードで動くことが求められているのです。

次を開始：
ランチパッドの処理待ち通知



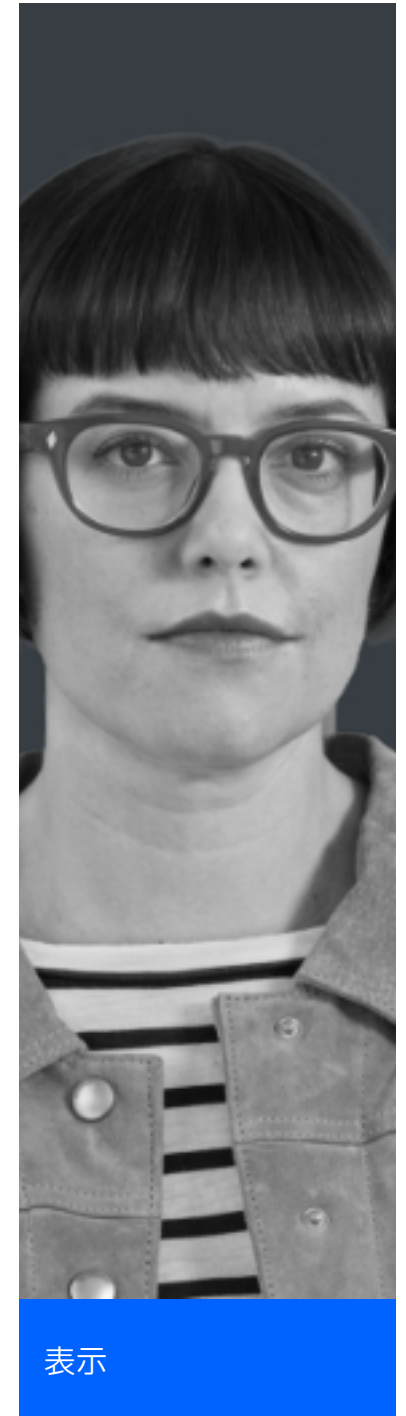
20%

IT ヘルプ・デスクへの問い合わせのうち、20% から 50% がパスワードの再設定に関するものです

世界経済フォーラム

「ただ仕事をしようとしているだけなのに、ツールやシステムに阻まれるのは、本当に苦痛です。」

Jacob、従業員



従業員



ビジネス管理職



アクセス権の
要求プロセス



IT 管理者



開発者



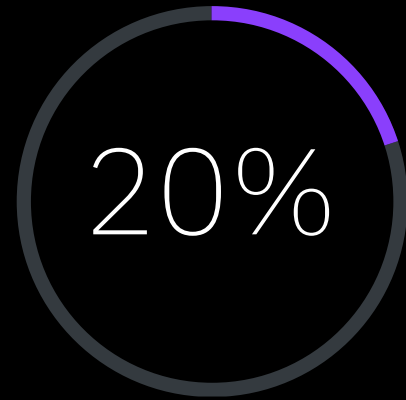
戻る

次へ

基幹業務の管理職

委任されたコントロールで、チーム固有のアプリケーションの権限付与を管理します。

基幹業務の管理職は、競争力を維持するために、新規サービスを従業員やお客様に迅速に提供する必要があります。IT の対応を待つことなく、ビジネスのスピードで動くことが求められているのです。



IT ヘルプ・デスクへの問い合わせのうち、20% から 50% がパスワードの再設定に関するものです

世界経済フォーラム

「ただ仕事をしようとしているだけなのに、ツールやシステムに阻まれるのは、本当に苦痛です。」

Jacob、従業員



ビジネス管理職



従業員



ビジネス管理職



アクセス権の要求プロセス



ランチパッドの処理待ち通知



要求の詳細を見る



追加の正当性の要求



要求の承認 / 拒否



IT 管理者



開発者

基幹業務の管理職 : 1 / 4

アクセス権の要求プロセス

ランチパッドの処理待ち通知

Jacob は、Bane & Dox Co. 社の販売チームの管理職です。IBM Security Verify にログインすると、アクセス可能なすべてのアプリケーションを見ることができます。Jacob は、組織のために DocuSign を管理し、IT の対応を待つことなく、従業員のアクセス要求を承認する権限を委任されました。ここでは、アプリの要求に対する処理待ち通知を見ることができます。

次は：
[要求の詳細を見る](#)



My apps

What app are you looking for?

Sort by A-Z

© 2020 Bane & Dox Co.



基幹業務の管理職 : 2 / 4

アクセス権の要求プロセス

要求の詳細を見る

Jacob はアプリケーションの要求のタブから、Jessica からのこの要求の詳細を見ることができます。必要であれば、提出された要求の正当性を追加で求めることもできます。

The screenshot shows the 'Task manager' interface for 'Bane & Dox Co.'. It features a navigation bar with 'App center', 'My requests', and 'Task manager'. The main content area is divided into 'App requests' and 'Access certification'. A table lists two requests for 'DocuSign' by Jessica Hudson and Joe Shmoe, both with a status of 'Need action' and a request date of '15th May 2020'. A right-hand panel titled 'Request details' provides information for the selected request, including the request ID, status, requester, request date, and a comment from Jessica Hudson: 'I need to sign sales contracts to close deals.' At the bottom of the panel are 'Reject' and 'Approve' buttons.

Requester	Name	Status	Request date	Last action
<input type="checkbox"/>	Jessica Hudson	Need action	15th May 2020	15th May 2020
<input type="checkbox"/>	Joe Shmoe	Need action	15th May 2020	15th May 2020

次は：
追加の正当性の要求



従業員

ビジネス管理職

アクセス権の
要求プロセス

IT 管理者

開発者



戻る

次へ

基幹業務の管理職 : 3 / 4

アクセス権の要求プロセス

追加の正当性の要求

その要求を送り返して、追加の正当性を求めることができます。

次は：
要求の承認／拒否



従業員



ビジネス管理職



アクセス権の
要求プロセス



IT 管理者



開発者

The screenshot displays the 'Task manager' interface for 'Bane & Dox Co.'. The main content area shows a table of 'App requests' with columns for Requester, Name, Status, Request date, and Last action. A dialog box titled 'Request justification' is overlaid on the table, prompting the user to provide a department code for billing purposes. The right sidebar shows 'Request details' for a DocuSign request, including the Request ID, Status (Need action), Requester (Jessica Hudson), Request date (15th May 2020), Last action (15th May 2020), and a comment from Jessica Hudson: 'I need to sign sales contracts to close deals.' At the bottom of the sidebar, there are 'Reject' and 'Approve' buttons.

基幹業務の管理職 : 4 / 4

アクセス権の要求プロセス

要求の承認 / 拒否

または、Jacob はリクエストを承認 / 拒否できます。直属の部下のアクセス承認権があるため、Jacob は IT ロジスティクスに負担を感じることなく、ビジネスのスピードに合わせた行動を取ることができるようになりました。

次は:
IT 管理者



従業員

ビジネス管理職

アクセス権の
要求プロセス

IT 管理者

開発者



戻る

次へ

IT 管理者

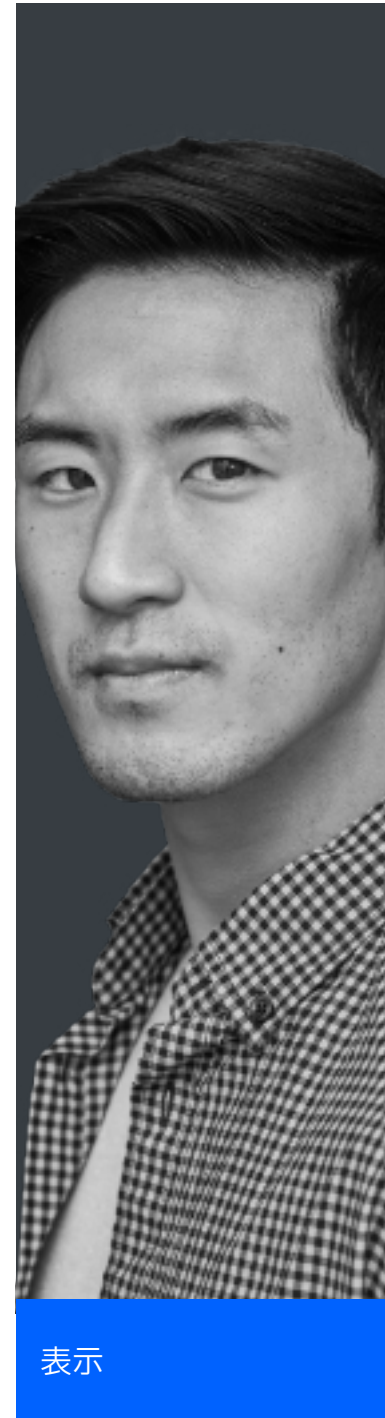
設定の簡素化、共通のプラットフォーム上での拡張、リスク保護の自動化。

IT 管理者は、時間、スキル、リソースの不足という環境の中で、認証情報の悪用から組織を保護する一方で、簡単なアクセスが求められるビジネス上の要求を満たす必要があります。また、さまざまなベンダーのクラウド・アプリケーションを取り入れると、制御が効かなくなることがあります。そのため、SSO(シングルサインオン)とMFA(多要素認証)のための統合ワークフローが最も重要になります。

次を開始：
ライブ・ダッシュボード



表示



表示

80%

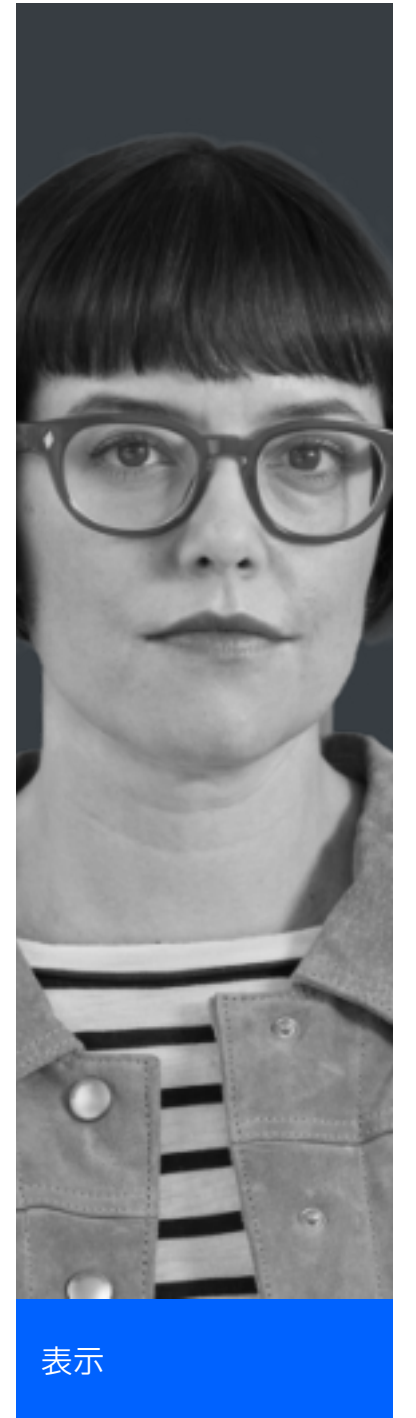
ハッキング関連の侵害の80%は、脆弱な認証情報の漏洩に関係しています

世界経済フォーラム

「組織の生産性を向上させ、同僚の安全を確保し、IDとアクセスに関するあらゆるリスクを考慮する必要があります。」

Scott、IT 管理者

IT 管理者



表示



従業員



ビジネス管理職



IT 管理者



活動の監視



ポリシーのカスタマイズ



ユーザーとIDの管理



アプリケーションの追加



リスクを分析

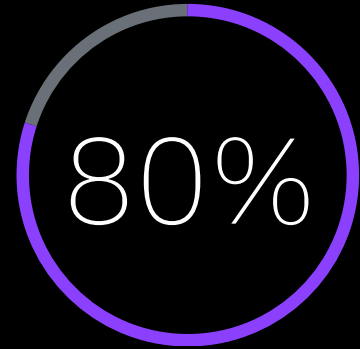


開発者

IT 管理者

設定の簡素化、共通のプラットフォーム上での拡張、リスク保護の自動化。

IT 管理者は、時間、スキル、リソースの不足という環境の中で、認証情報の悪用から組織を保護する一方で、簡単なアクセスが求められるビジネス上の要求を満たす必要があります。また、さまざまなベンダーのクラウド・アプリケーションを取り入れると、制御が効かなくなることがあります。そのため、SSO(シングルサインオン)とMFA(多要素認証)のための統合ワークフローが最も重要になります。



ハッキング関連の侵害の 80% は、脆弱な認証情報の漏洩に関係しています

世界経済フォーラム

「組織の生産性を向上させ、同僚の安全を確保し、ID とアクセスに関するあらゆるリスクを考慮する必要があります。」

Scott、IT 管理者



IT 管理者



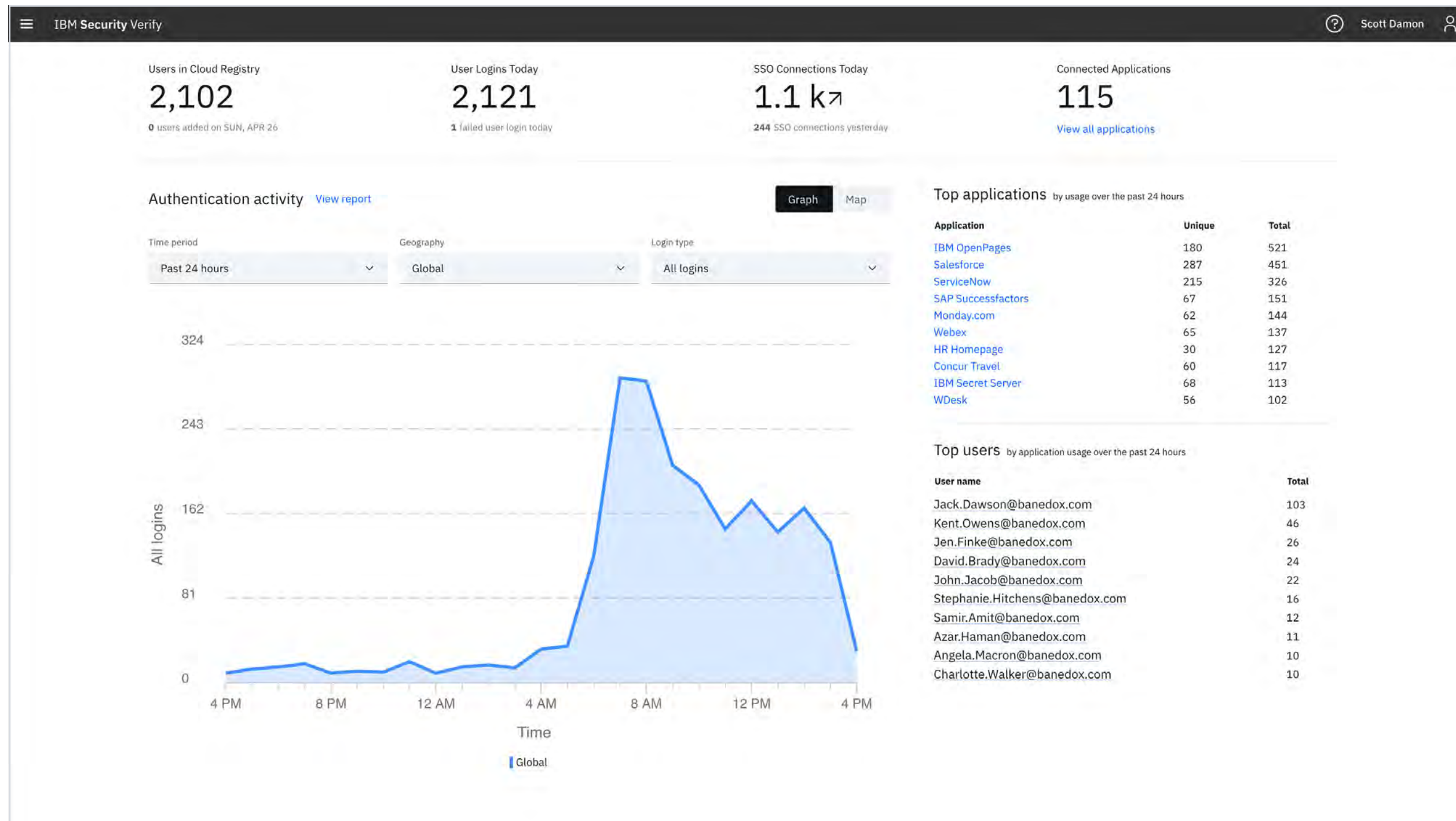
IT 管理者 : 1 / 3

活動の監視

ライブ・ダッシュボード

IBM Security Verify の管理用ダッシュボードでは、組織内の認証活動のグローバルな概要を表示できます。IT 管理者である Scott は、期間や地域で絞り込んで、ユーザーの動向をより詳しく把握できます。

次は：
活動レポートの作成



従業員

ビジネス管理職

IT 管理者

活動の監視

ポリシーのカスタマイズ

ユーザーとIDの管理

アプリケーションの追加

リスクを分析

開発者



戻る

次へ

IT 管理者 : 2 / 3

活動の監視

活動レポートの作成

Verify のレポート作成インターフェースにより、Scott は最近の活動データをライブで絞り込んで、問題を迅速に診断できます。認証活動、適応型アクセス、アプリケーション使用状況、管理者活動、および MFA(多要素認証) 活動など、組織のアクセスと認証データを深く掘り下げ、インサイトを収集し、事象のトラブルシューティングを行うことができます。

次は：
[適応型アクセス活動レポート](#)

Reports

- Authentication activity**
All Cloud Identity sign-in attempts for a given time range.
View Report
Successful logins: 2.1k, Failed logins: 5
Past 24 hours
- Adaptive access**
All access attempts regulated by an adaptive access policy.
View Report
Very high: 5, High: 27, Medium: 48, Low: 1.1k
Past 24 hours
- Application usage**
Sign-in attempts for an application for a given time range.
Select application: All applications
View Report
- Admin activity**
Management events performed by admin users and application owners.
Latest activity:
- few seconds ago: Box application modified
- 1 hour ago: Monday.com application deleted
- 1 hour ago: Monday application deleted
View Report
- MFA activity**
Multi-factor authentication activity by method
Top used MFA factors:
SMS OTP: 125, Email OTP: 220, TOTP: 31, IBM verify push: 175
Past 30 days
View Report
- Fulfillment activity**
Provisioning and de-provisioning operations for an application for a specified time range.
Select application: All applications
View Report



従業員



ビジネス管理職



IT 管理者



活動の監視



ポリシーのカスタマイズ



ユーザーと ID の管理



アプリケーションの追加



リスクを分析



開発者



戻る

次へ

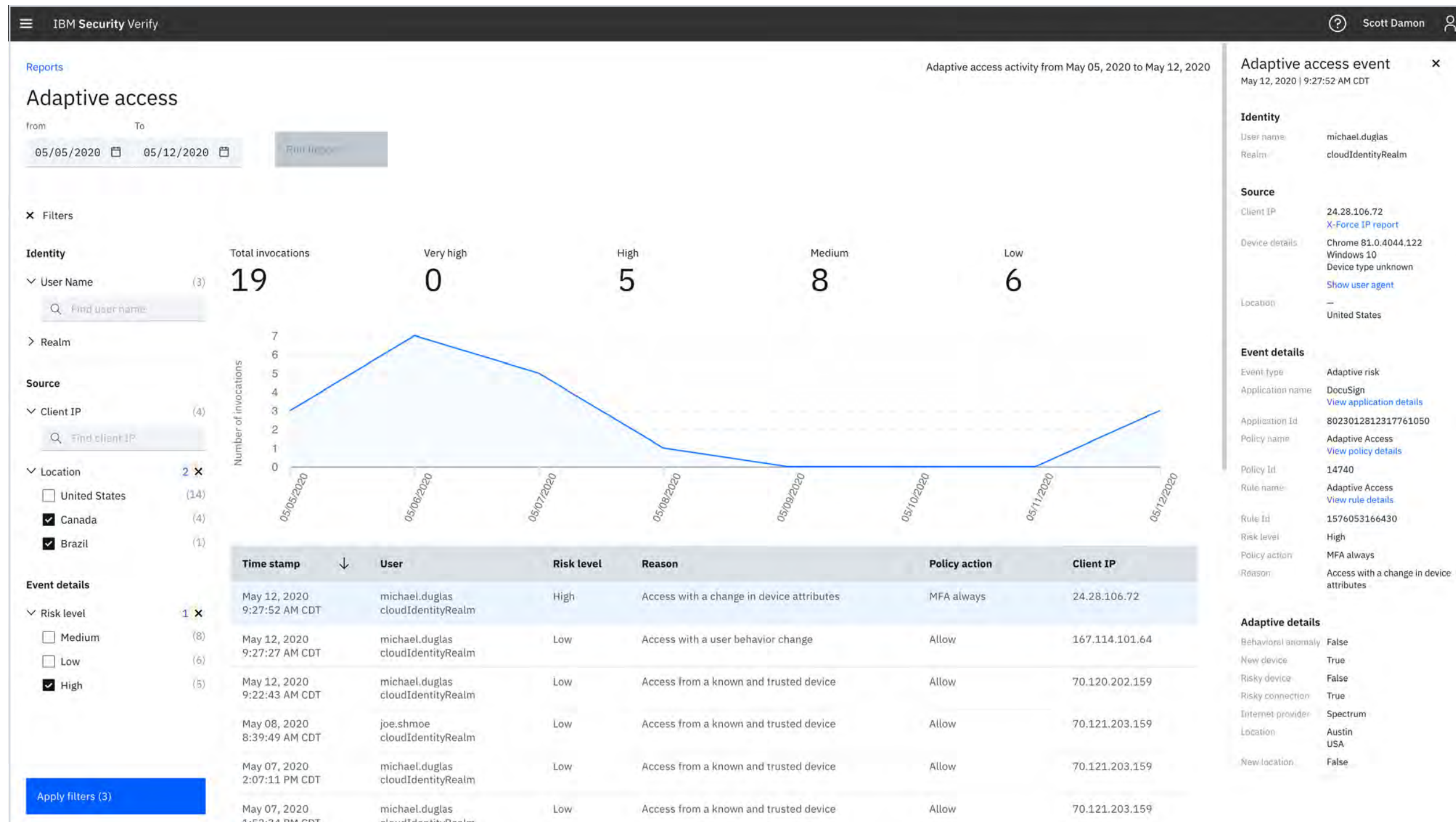
IT 管理者 : 3 / 3
活動の監視

適応型アクセス 活動レポート

例えば、適応型アクセスのレポートでは、適応型アクセスのポリシーと文書化されたイベント・パラメーターを使用したアプリケーションから、最近のすべてのログインを確認できます。Verify のレポートを使って、リスクの高い事象を診断し、トラブルシューティングを行い、必要であれば対策を講じることができます。

適応型アクセスのインタラクティブ・デモ

次は：
ポリシーのエディター



従業員

ビジネス管理職

IT 管理者

モニター
アクティビ
ティ

ポリシーの
カスタマイズ

ユーザーと
ID の管理

アプリケーション
の追加

リスクを
分析

開発者



戻る

次へ

IT 管理者 : 1 / 3
 ポリシーのカスタマイズ

ポリシーのエディター

アクセス・ポリシーのエディターでは、組織のアプリケーションで使用する追加のカスタム・アクセス・ポリシーを作成できます。一部のポリシーはデフォルトで含まれています。例えば、常にアクセスを許可する、常に二要素認証 (2FA) を要求する、新規セッションの開始時に 2FA を要求するなど、があります。

次は：
ポリシーにルールを追加



The screenshot shows the IBM Security Verify Policy Editor interface. At the top, there's a navigation bar with 'IBM Security Verify' and a user profile 'Scott Damon'. Below that, a 'Security' section contains several tabs: 'Access policies', 'Authentication factors', 'FIDO2', 'Registration profiles', 'Tokens', 'Application consents', 'Policy editor' (which is active), and 'Sign-in options'. Under 'All policies', there's a table listing various policies with their descriptions and edit/delete icons. An 'Add policy' button is visible in the top right of the table area.

Policy name	Policy description	
Corporate access policy	Global policy check	
Corporate network policy	Only allow access when on the corporate VPN	
Enable 2fa bypass on specific IP range	When an external IP in the range is matched, then 2FA will not be required. Otherwise, 2FA will be required.	
Master Policy		
MFAGroup Policy	Remove ability to talk to apple	
Require 2FA on Android only	Require 2FA for Android devices.	
Trusteer Device Policy	Use the Trusteer recommendation to determine the 2FA requirements for the session.	
Allow access from all devices	Allow users to access from desktops, including laptops and Microsoft tablets, and from mobile devices. The mobile device can be managed or unmanaged by IBM MaaS360. The managed mobile device can be compliant or non-compliant to the IBM MaaS360 IT policy.	
Allow access from desktops and managed mobile devices; block otherwise	Allow users to access from desktops and from managed mobile devices. Deny access from unmanaged mobile devices.	
Allow access from compliant devices only; others require 2FA	Allow users to access from compliant managed devices. If users access from unmanaged or non-compliant managed devices, the users must complete a second factor authentication every time the users access an application from these devices.	
Allow access from compliant devices only; others require 2FA each session	Allow users to access from compliant managed devices. If users access from unmanaged or non-compliant managed devices, prompt users to complete a second factor authentication one-time, on the first access attempt in an authenticated session with IBM Security Verify.	
Allow access from compliant devices only; block otherwise	Allow users to access from compliant and managed devices only.	
Allow access from desktops and compliant mobile devices; block otherwise	Allow users to access from desktops and from compliant managed mobile devices. Deny access from unmanaged and non-compliant managed mobile devices.	
Allow access from compliant mobile devices only; always require 2FA in	Allow users to access from compliant managed mobile devices. If users access from desktops, the users must complete a second-factor authentication every time the users access an	



IT 管理者 : 2 / 3
ポリシーのカスタマイズ

ポリシーに ルールを追加

Scott は、デバイス、グループ・メンバー、IP と地理的位置情報などの条件に基づいて、アクセス権または MFA(多要素認証) によるチャレンジを許可またはブロックするルールを簡単に設定できます。

次は：
適応型アクセス

The screenshot displays the 'Policy rule' configuration page in the IBM Security Verify console. The rule is titled 'Unknown device and geographic location'. It consists of two conditions connected by 'And': 'New device' (Condition type: Device type, Operation: Is, Value: Detected) and 'Location history' (Condition type: Location history, Operation: Is, Value: Check location history). The action is 'MFA always'. Under 'Authentication methods', 'FIDO2', 'Time-based OTP', and 'IBM Verify' are checked. The interface includes a sidebar with 'Security' and 'All policies' sections, and a bottom navigation bar with 'Back' and 'Next' buttons.



IT 管理者 : 3 / 3

ポリシーのカスタマイズ

適応型アクセス

また、適応型アクセス・ポリシーによってリスク・ベース認証を有効にし、ユーザー、デバイス、活動、環境、および行動の詳しいコンテキストを自動的に考慮することも可能です。適応型アクセスでは、AI を活用した堅牢なコンテキスト・パラメーターのセットで全体的なリスク・レベルが決定されます。継続的な認証により、低リスクのユーザーには摩擦のないアクセスが与えられ、高リスクのユーザーには自動的にチャレンジまたはブロックが行われます。

適応型アクセスのインタラクティブ・デモ

次は：
管理職ユーザー

The screenshot displays the 'Policy rule' configuration page in the IBM Security Verify console. The rule is titled 'Unknown device and geographic location'. It features two conditions: 'If New device Is Detected' and 'And Location history Is [operation]'. The action is configured as 'MFA always' with the following authentication methods selected: FIDO2, Time-based OTP, and IBM Verify. The interface includes a sidebar with navigation options like 'Security', 'Access policies', and 'All policies'. At the bottom of the configuration window, there are 'Back' and 'Next' buttons.



従業員

ビジネス管理職

IT 管理者

活動の監視

ポリシーの
カスタマイズ

ユーザーと
ID の管理

アプリケーション
の追加

リスクを
分析

開発者



戻る

次へ

IT 管理者 : 1 / 5
ユーザーと ID ソースの管理

管理職ユーザー

Scott は、シンプルな構成インターフェースで新規ユーザーを取り込むことができます。また、ゼロから属性を追加すること、またはクラウド・ディレクトリー、Active Directory、IBMid など、さまざまな ID ソースからデータを取り込むことも可能です。

次は：
グループの管理

The screenshot displays the 'Policy rule' configuration page in the IBM Security Verify console. The left sidebar shows a navigation menu with 'Security' and 'Access policies' sections. The main content area is titled 'Policy rule' and includes a description: 'When all conditions are met the action will be enforced during authentication.' The rule name is 'Unknown device and geographic location'. The rule is configured with two conditions: 'If New device Is Detected' and 'And Location history Is [blank]'. The action is 'Then MFA always'. Under 'Authentication methods', 'FIDO2', 'Time-based OTP', and 'IBM Verify' are selected. The interface includes 'Back' and 'Next' buttons at the bottom right.



IT 管理者 : 2 / 5

ユーザーと ID ソースの管理

グループの管理

部署別、役割別、あるいはもっと固有の属性で編成されているかどうかにかかわらず、グループは組織内のアクセスをさらにモジュール化できます。例えば、Scott は新規で Bane & Dox Co. 社の営業グループを追加して、個々人の集合が共通の営業アプリケーションにアクセスする支援ができます。既存のディレクトリーを Verify に統合すると、そのディレクトリーのグループが保持されます。

次は：
ユーザー属性の管理

The screenshot shows the IBM Security Verify interface. The main view is 'Users & groups' with a 'Groups' tab selected. A modal window titled 'Edit Group' is open, showing details for the 'Enablement' group. The modal includes the following information:

- Name***: Enablement
- Description**: A group for our enablement team
- Date Created**: 5/20/2019
- Date Modified**: 5/20/2019
- Group Members**: A list of users including Indiana Ham, Iris Challoner, Isaac Cary, Isaac Hosford, Jade Bradford, Jade Lincoln, Jade Monteith, Jaime Haverill, James Inledon, and Janel Challoner.

Buttons for 'Add', 'Delete', 'Add Members', and 'Remove Members' are visible. The background shows a list of other groups like 'admin', 'ADSyncAdmins', 'ADSyncBrows...', etc.



IT 管理者 : 3 / 5

ユーザーと ID ソースの管理

ユーザー属性の管理

Verify には、デフォルトで最も一般的なユーザー属性が数十項目含まれていますが、必要に応じて、接続された ID ソースのいずれかから追加の属性をリンクさせること、またはカスタム属性を作成できます。これらの属性はその後、シングル・サインオン、プロビジョニング、プロフィールの作成などのために、ID ソースとアプリケーションで参照できます。

次は :
Active Directory と LDAP

The screenshot displays the 'Edit attribute' configuration interface in IBM Security Verify. The left sidebar shows a list of attributes, with 'costcenter' selected. The main content area is divided into three sections: 'Name and description', 'Availability', and 'Source and value'. In the 'Name and description' section, the attribute name is 'costcenter' and the description is 'Cost center attribute for billing purposes'. The 'Availability' section has 'Single sign-on (SSO)' checked under 'Make available for (select all that apply)'. The 'Source and value' section shows a table with one entry: 'Active Directory' as the identity source and 'department' as the attribute name from the identity source. At the bottom right, there are 'Cancel' and 'Save' buttons.



従業員

ビジネス管理職

IT 管理者

活動の監視

ポリシーの
カスタマイズ

ユーザーと
ID の管理

アプリケーション
の追加

リスクを
分析

開発者



戻る

次へ

IT 管理者 : 4 / 5
ユーザーと ID ソースの管理

Active Directory と LDAP

Scott は、既存の Active Directory や LDAP ID ソース、あるいは非標準のディレクトリー、データベース、外部サービスに接続するように Verify を構成できます。

次は：
ソーシャル・ログイン

The screenshot shows the 'Edit attribute' configuration interface in IBM Security Verify. The left sidebar lists various attributes, with 'costcenter' selected. The main content area is divided into sections: 'Name and description' (Attribute name: costcenter, Description: Cost center attribute for billing purposes), 'Availability' (Single sign-on (SSO) checked), and 'Source and value' (Identity source: Active Directory, Attribute name from the identity source: department). A 'Save' button is highlighted in blue at the bottom right.



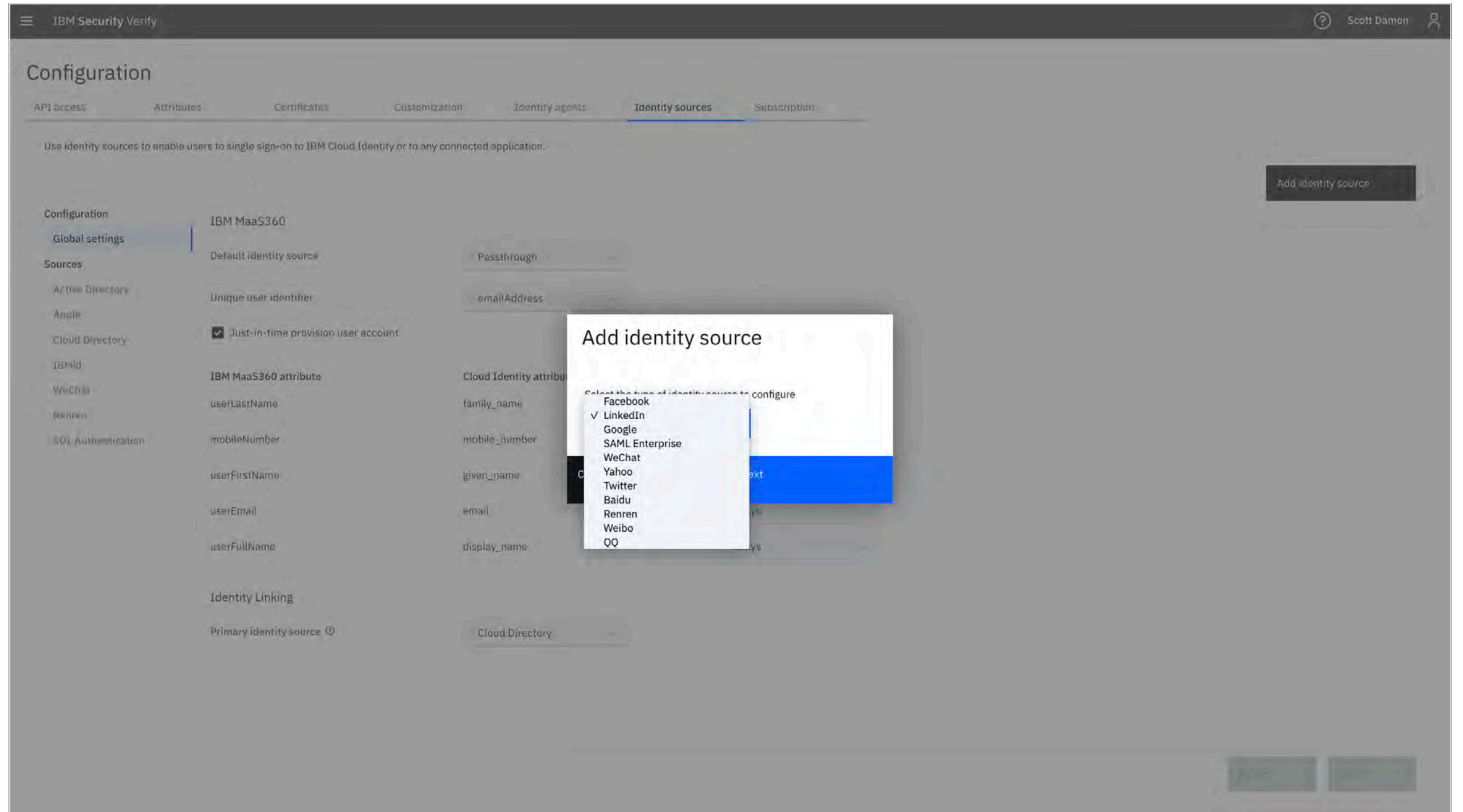
IT 管理者 : 5 / 5

ユーザーと ID ソースの管理

ソーシャル・ログイン

また、Google と LinkedIn、地域別のプロバイダーなど、さまざまなソーシャル・ログイン・プロバイダーをリンクさせ、ユーザーにより多くの選択肢を提供することも可能です。

次は：
アプリケーションの表示



従業員



ビジネス管理職



IT 管理者



活動の監視



ポリシーのカスタマイズ



ユーザーと ID の管理



アプリケーションの追加



リスクを分析



開発者



戻る

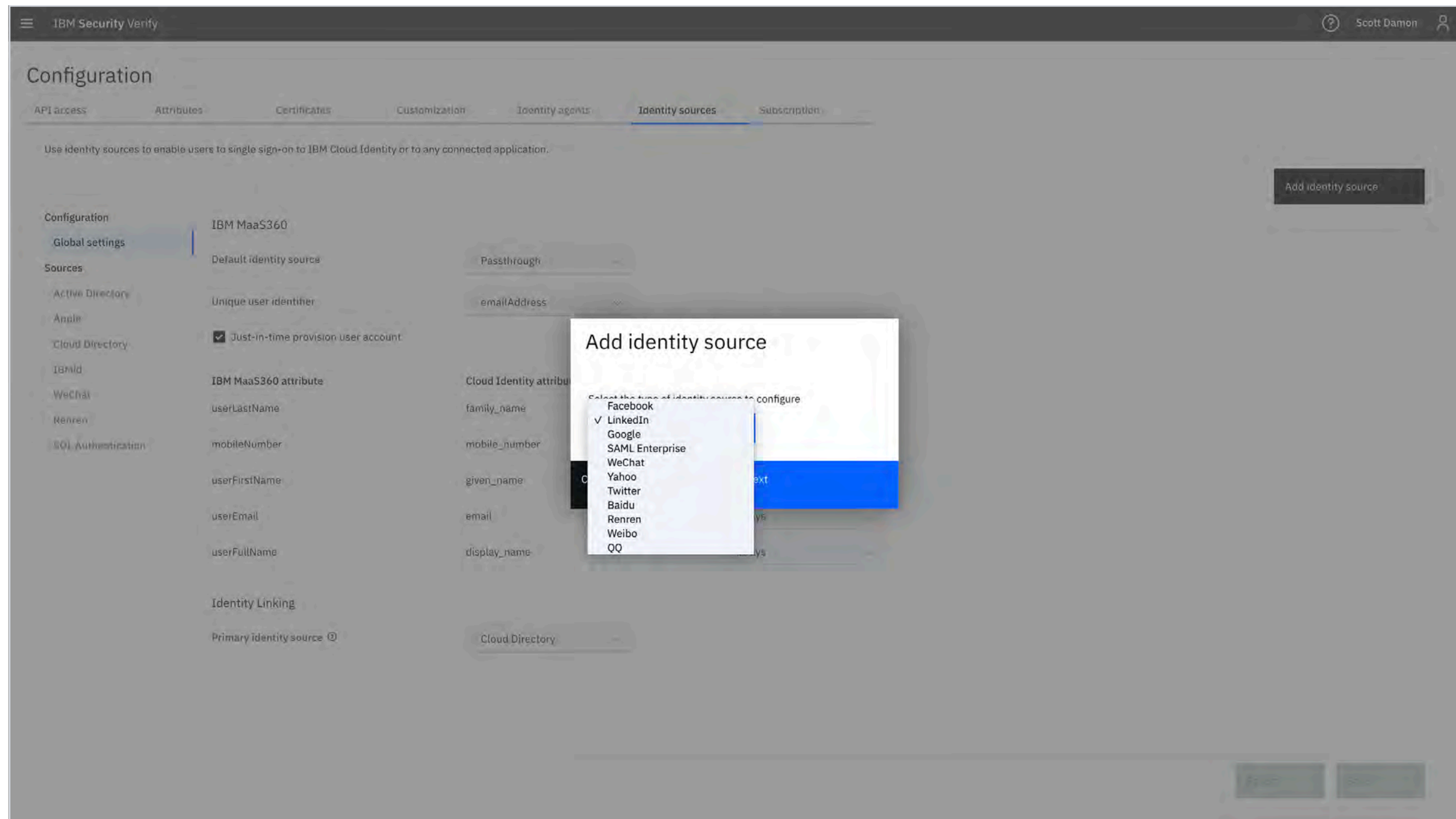
次へ

IT 管理者 : 1 / 6
アプリケーションの追加

アプリケーションの表示

Verify では、数百に上る SaaS アプリケーションにそのまますぐに対応します。また、カスタム・アプリケーションの合理的な統合が可能で、オンプレミス・アプリケーションにも対応を拡張する、軽量のアプリケーション・ゲートウェイが提供されています。Scott は、組織のすべてのアプリケーションを単一のインターフェイスから管理できます。

次は：
追加するアプリケーションの検索



従業員

ビジネス管理職

IT 管理者

活動の監視

ポリシーの
カスタマイズ

ユーザーと
ID の管理

アプリケーション
の追加

リスクを
分析

開発者



戻る

次へ

IT 管理者 : 2 / 6
アプリケーションの追加

追加する アプリケーションの 検索

Scott は、Monday.com のように、追加する新規アプリケーションを検索できます。SaaS コネクタが事前に組み込まれているため、新規アプリケーションを統合型シングル・サインオンとして統合することは簡単です。

次は：
アクセス権承認のために
オーナーを追加

The screenshot shows the IBM Security Verify 'Applications' page. At the top, it displays 'Total applications: 24' and 'Enabled: 24'. A modal window titled 'Select Application Type' is open, showing a search bar and a list of application templates. The selected application is 'Monday.com', described as 'A visual project management tool that helps transform the way teams work together'. Other visible templates include Custom Application, mingie by 1noughtworks, Miro, mixpanel, MODE, Mojohelpdesk, Mozy, and Mulesoft. The background shows a list of applications with columns for Type, Name, and Enabled status.



IT 管理者 : 3 / 6

アプリケーションの追加

アクセス権承認のためにオーナーを追加

アプリケーションの継続的な運用を管理するために、Scott はアクセス権要求のために、アプリケーションのオーナーとアクセス権の承認者を割り当てることができます。

次は：
サインオン設定の構成



従業員

ビジネス管理職

IT 管理者

活動の監視

ポリシーのカスタマイズ

ユーザーとIDの管理

アプリケーションの追加

リスクを分析

開発者

IBM Security Verify

Scott Damon

Add Application

Monday.com

Monday.com

General Sign-on

Settings

- Enabled
- Show on launchpad

Description

A visual project management tool that helps transform the way teams work together.

Company name*

monday.com

Account name*

Client

Use the 'Account Name' from the monday.com Admin > General > Profile page.

Application owners

Add owner

Jacob Alexander
jacob@banedox.com
jacob@banedox.com@cloudIdentityRealm

Summary

X-Force Details
[View in X-Force Exchange](#)

Categorization
Cloud, Software as a Service

Description
A visual project management tool that helps transform the way teams work together

Base URL
http://monday.com/

Risk Score
0.1

Cancel Save



戻る

次へ

IT 管理者 : 4 / 6

アプリケーションの追加

サインオン設定の構成

サインオン・タブでは、アプリケーションと Verify との適切な統合のために必要なパラメーターが構成できます。また、アプリケーション固有の説明書もヘルプとして用意されています。さらにこのページの下部では、サービス・プロバイダーに送信する属性のマッピングや、アプリケーションに適用するアクセス・ポリシーなど、統合の他の側面が設定できます。

次は：
権限付与の構成

The screenshot shows the 'Add Application' configuration page for Monday.com. The main form is divided into sections: General, Sign-on, SAML subject, Just-in-time provisioning, and Attribute mappings. The Sign-on section includes fields for Provider ID* and Assertion consumer service URL (HTTP-POST)*, both set to `https://banedox.monday.com/saml/saml_callback`. The SAML subject section has a Name identifier set to `preferred_username`. The Attribute mappings section has a table with columns for Attribute name, Attribute name format, and Attribute source.

Attribute name	Attribute name format	Attribute source
Email*	<code>urn:oasis:names:tc:SAML:2.0:attrname-format:basic*</code>	Select attribute source
FirstName*	<code>urn:oasis:names:tc:SAML:2.0:attrname-format:basic*</code>	Select attribute source

The right-hand sidebar contains a section titled 'monday.com SAML2.0 single sign-on (SSO) configuration'. It lists prerequisites and a 5-step configuration guide:

- Log in as an admin user to your monday.com account using the following URL: `https://<monday.com Account Name>.monday.com/users/sign_in`
- Click your profile name and then select **Admin** from the drop-down menu.
- Click **Security**.
- On **Login** page, click **Open** next to the **SAML** option.
- In the **Security & Authentication Settings** section, specify the following settings:
 - SAML SSO Url**: `https://rlshahatestmobile.itel.idmg.ibmcloudsecurity.com/saml/sp#/saml20ip/saml20/login`

At the bottom of the sidebar, it states: 'If the **Use unique ID** check box is selected, use the following value:'. The main form has 'Cancel' and 'Save' buttons at the bottom right.



従業員

ビジネス管理職

IT 管理者

活動の監視

ポリシーのカスタマイズ

ユーザーと ID の管理

アプリケーションの追加

リスクを分析

開発者



戻る

次へ

IT 管理者 : 5 / 6
アプリケーションの追加

権限付与の構成

権限付与のタブでは、アプリケーションに適したアクセスおよび承認ロジックのレベルが設定できます。この場合は、特定のユーザーとグループのセットを選択します。

次は：
定期的なアクセス再認証の設定



IT 管理者 : 6 / 6
 アプリケーションの追加

定期的なアクセス再認証の設定

時間の経過とともに、組織としてアクセス・レベルが依然として適切であることの確認が困難になる場合があります。この重要なステップを見逃さないために、アプリケーションごとに定期的な再認証キャンペーンを設定すれば、ID ガバナンスのこの側面を自動化できます。

次は：
 分析ダッシュボード



The screenshot shows the 'Productivity applications' campaign configuration page in IBM Security Verify. The page is titled 'Governance / Certification campaigns' and 'Productivity applications'. It features a 'Running' status indicator and a 'Pause' button. The configuration is divided into several sections:

- General settings and scope:**
 - Name: Productivity applications
 - Description: All cloud based productivity applications
 - Type: User entitlement
 - Priority: Medium
 - Applications: Atlassian, Box, Clever, Monday
 - Include only: All users and groups included
 - Except for: Enablement
 - Reviewer: User manager
- Schedule:**
 - Start date: April 27, 2020 5:24:56 PM CDT
 - Duration: 30 days
 - Frequency: This campaign repeats every 3 months (with a link to 'View upcoming dates')
- Campaign end:**
 - Reminders: Start 10 days before the campaign ends
 - Campaign end: Take no action on entitlements not reviewed
- Details:**
 - Campaign ID: d5fc1070a8c0425da210ab60cc216516
 - Created by: Scott Damon (scott.damon@banedox.com, scott@cloudIdentityRealm)
 - Created on: Apr 27, 2020
 - Modified on: -



IT 管理者 : 1 / 3
リスクを分析

分析ダッシュボード

ID 分析ダッシュボードでは、組織の IAM(アイデンティティ・アクセス管理)の全体的な健全性を確認でき、ユーザー、権限付与、アプリケーションの ID 関連のリスクを迅速に精査できます。また、個々のユーザーやアプリケーションを深く掘り下げることで、違反行為や蓄積されたリスク・スコアをさらに詳しく把握できます。

次は：
ポリシー違反のランキングを表示



IBM Security Verify ? Scott Damon

Quick insights Last analysed on 16 Dec 2019, 15:42:34

Risky users

110

Critical violations

264

Risky applications

15

Risky entitlements

76

Top recommended actions

Pending reviews

721

All violations

739

Recertify access
Suspend account

Top high risk violations

High risk violations

- Access is never recertified
- Account is dormant
- Person is suspended but one or mor...
- User's entitlement deviates from p...
- Account is orphan

Top risky applications All applications

Score ↓	Type	Application	Severity ⓘ
175.98		Zolo CRM	
45.47		JKFinance	
39.81		StoreLinux	
37.95		MayuriLinux	
36.22		ITIM Service	
27.38		Linux_sued	
24.94		Dusty	
22.72		PGLinux	
19.3		Sales Composer	
15.13		IGI	
13.48		Mina	

Top risky users All users

Score ↓	User	Severity ⓘ
11.59	Alan Smith	
11.25	Bhattacharjee	
10.61	Chuck Riegler	
10.6	Kevin Nolan	
10.38	Mason Mount	

Top violations All violations

Score ↓	Violation	Severity ⓘ
164.97	User's entitlement deviates from peers	
144.2	Access is never recertified	
112.7	Account is orphan	
31	Access was not added through workflow approval	
28	Person is suspended but one or more of their accounts are not suspended	

○ 従業員

○ ビジネス管理職

● IT 管理者

● 活動の監視

● ポリシーのカスタマイズ

● ユーザーと ID の管理

● アプリケーションの追加

● リスクを分析

○ 開発者

IT 管理者 : 2 / 3

リスクを分析

ポリシー違反のランキングを表示

例えば、「ユーザーの権限付与のピアからの逸脱」という観点では、ポリシーのカテゴリ内の異常を強調し、違反をランク付けして表示できます。この特定のポリシーは、ID 分析においてピア・グループ分析を行い、追加的なリスクをもたらす可能性のある、非典型的な権限付与を特定するものです。

次は：
提案された修復措置の実行

IBM Security Verify

← Back to dashboard

Application Search

User's entitlement deviates from peers

Critical violations: **118** | High risk violations: **45** | All violations: **174**

In peer group **Organization Name (Sales Organization)**, only **0.85%** users are entitled to use Access Report.

Score ↓	User	Application	Entitlement	First Occurrence	Last Occurrence				
0.99	Alan Smith	JKFinance	Access Report	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	99.15%
0.99	Rob Hulse	Peckers	Finance_Tools	16 Dec 2019, 15:18:15	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI	94.29%
0.99	Chuck Riegler	ISIM - isim_aditya	Offering Manager	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	98.51%
0.99	Josh King	Linux_sued	slocate	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	93.8%
0.99	Joe Murphy	StoreLinux	audio	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	99.58%
0.99	Charles Robert	ISIM - isim_aditya	TestDynamicRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	98.62%
0.99	Steve Bruce	ISIM - isim_aditya	ManagerRole	11 Dec 2019, 12:25:18	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	92.39%
0.99	Trent Boulton	-	TestRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI	95.03%
0.99	Taylor Blackett	ISIM - isim_aditya	BlackettRole	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	94.42%
0.99	Chuck Riegler	JKFinance	TestGroup4	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	98.51%
0.99	Ladley King	Dusty	audio	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	98.9%
0.99	Callum Roberts	Linux2	cdrom	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	99.58%
0.99	Girish Chafle	Mina	adm	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	99.58%
0.99	Yogesh Kodgule	PGLinux	abrt	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	██████████	Recertify access	IGI,ISIM	99.49%



従業員

ビジネス管理職

IT 管理者

活動の監視

ポリシーのカスタマイズ

ユーザーと ID の管理

アプリケーションの追加

リスクを分析

開発者



戻る

次へ

IT 管理者 : 3 / 3
リスクを分析

提案された修復措置の実行

Verify ではまた、ポリシー違反の場合には、AI を活用したリスクと信頼度のスコアとともに、アクセス権の再認証などの改善策が提案されます。再認証の要求は ID 分析ダッシュボード内から実行できます。

次は：
開発者



IBM Security Verify ? Scott Damon

[← Back to dashboard](#) Application Search

User's entitlement deviates from peers

Critical violations

118

High risk violations

45

All violations

174

Score ↓	User	Application	Entitlement	First Occurrence	Last Occurrence	Severity	Recommended Action	Source	Confidence	
0.99	Alan Smith	JKFinance	Access Report	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	99.15%	
0.99	Rob Hulse	Peckers	Finance_Tools	16 Dec 2019, 15:18:15	16 Dec 2019, 15:18:15	■	Recertify access	IGI	94.29%	
0.99	Chuck Riegler	ISIM - isim_aditya	Offering Manager	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	98.51%	
0.99	Josh King	Linux_sued	slocate	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	93.8%	
0.99	Joe Murphy	StoreLinux	audio	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	99.58%	
0.99	Charles Robert	ISIM - isim_aditya	TestDynamicRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	98.62%	
0.99	Steve Bruce	ISIM - isim_aditya	ManagerRole	11 Dec 2019, 12:25:18	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	92.39%	
0.99	Trent Boulton	-	TestRole	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	■	Recertify access	IGI	95.03%	
0.99	Taylor Blackett	ISIM - isim_aditya	BlackettRole	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	94.42%	
0.99	Chuck Riegler	JKFinance	TestGroup4	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	98.51%	
0.99	Ladley King	Dusty	audio	16 Dec 2019, 11:28:55	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	98.9%	
0.99	Callum Roberts	Linux2	cdrom	10 Dec 2019, 15:47:47	16 Dec 2019, 15:18:15	■	Recertify access	IGI,ISIM	99.58%	

1 of 30 Selected.
Cancel
Add exception
Mark actioned
Recertify access



戻る

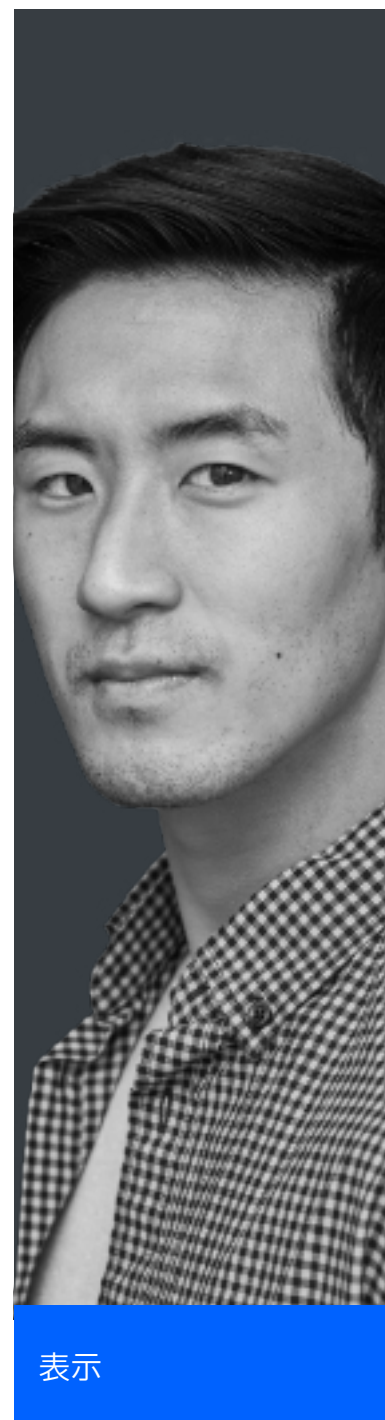
次へ

開発者

直感的な専用 API を使用して、カスタム・アプリケーションにアクセスと認証を組み込むことができます。

開発者は、認証のためのランタイム・フローを構築し、ユーザーに登録機能を与えて、アプリケーションに MFA(多要素認証)を埋め込む必要があります。開発者は、必ずしも IAM(アイデンティティ・アクセス管理)の専門家である必要はありません。これを効率的に行うには、堅牢な API と文書、サンプル・コード、ガイド付きインストラクションが必要です。

次を開始：
開発者ポータル



2024 年までには、アクセス管理ソリューションによる全アプリケーションへのアクセスの 70% 以上が MFA(多要素認証)を活用するようになります

ガートナー

「私が実際に達成しようとしていることにとって、このステップが障害になることがないように、認証を私のアプリケーションにすばやく組み込む必要があります」

Alice、開発者

開発者



従業員



ビジネス管理職



IT 管理者



開発者



開発者向け
リソース



カスタム・
アプリケーション
の構築



API の構成



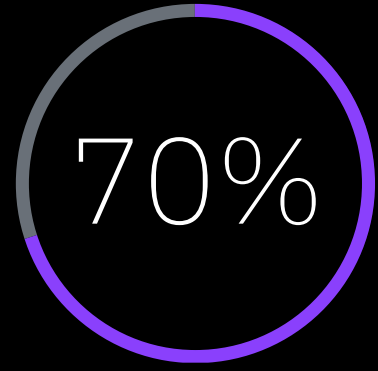
戻る

次へ

開発者

直感的な専用 API を使用して、カスタム・アプリケーションにアクセスと認証を組み込むことができます。

開発者は、認証のためのランタイム・フローを構築し、ユーザーに登録機能を与えて、アプリケーションに MFA(多要素認証)を埋め込む必要があります。開発者は、必ずしも IAM(アイデンティティ・アクセス管理)の専門家である必要はありません。これを効率的に行うには、堅牢な API と文書、サンプル・コード、ガイド付きインストラクションが必要です。



2024 年までには、アクセス管理ソリューションによる全アプリケーションへのアクセスの 70% 以上が MFA(多要素認証)を活用するようになります

ガートナー

「私が実際に達成しようとしていることにとって、このステップが障害になることがないように、認証を私のアプリケーションにすばやく組み込む必要があります」

Alice、開発者



開発者



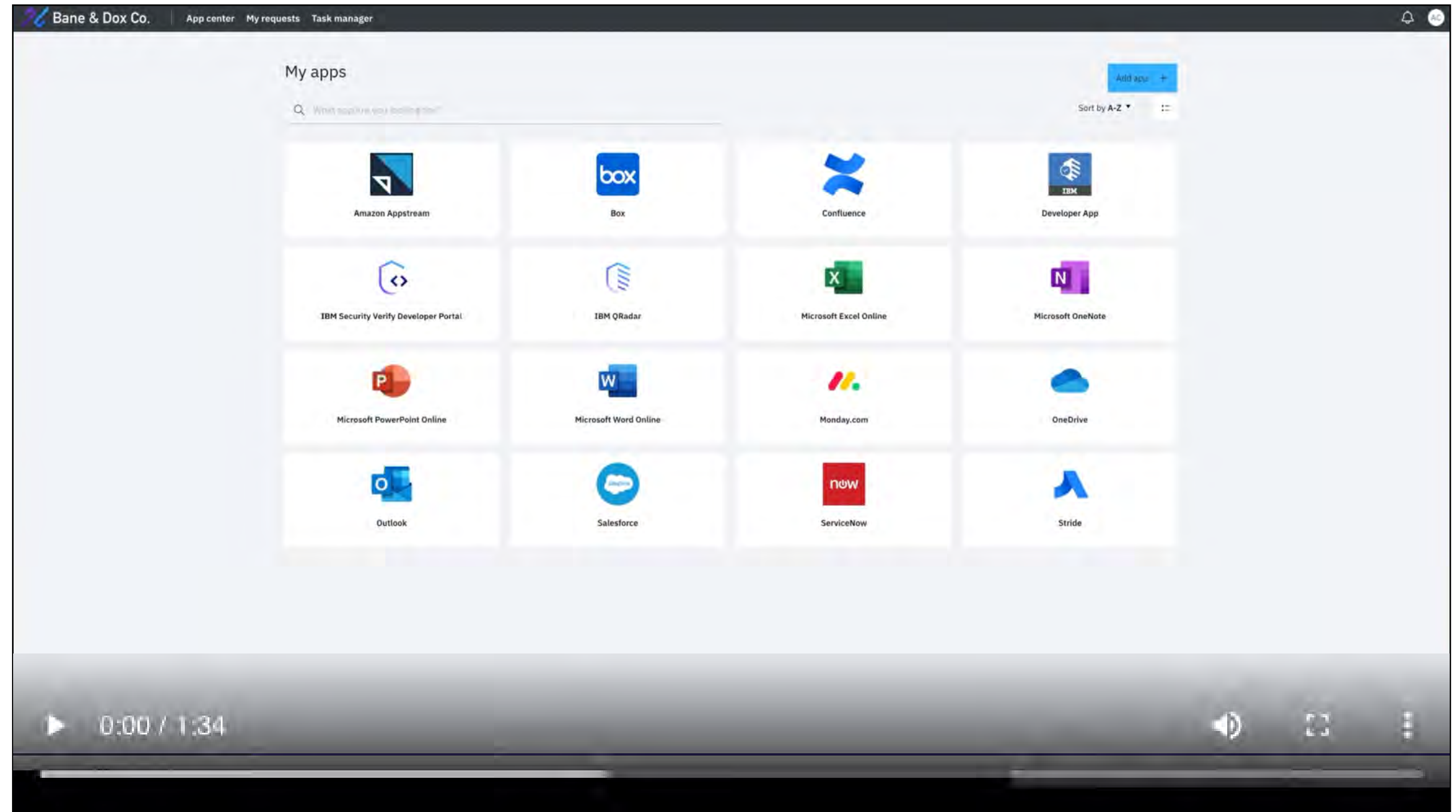
- 従業員
- ビジネス管理職
- IT 管理者
- **開発者**
- 開発者向けリソース
 - 開発者ポータル
 - API ヘルプ
- カスタム・アプリケーションの構築
 - カスタム・アプリケーションのテンプレートの追加
 - サインオン設定の構成
 - プロビジョニングの構成
 - バグのトラブルシューティング
- API の構成
 - API クライアントの追加
 - 委任管理

開発者 : 1 / 2
開発者向けリソース

開発者ポータル

IBM Security Verify の開発者ポータルでは、アプリケーションの統合プロセスのガイダンスが、ウィザードのような形態で開発者に提供されます。このポータル・サイトでは、標準的な API 文書に加え、コード・スニペット、段階的の手順、サンプル・アプリケーションを提供しています。

次は：
[API ヘルプ](#)



従業員



ビジネス管理職



IT 管理者



開発者



開発者向け
リソース



カスタム・
アプリケーション
の構築



API の構成



開発者 : 2 / 2
開発者向けリソース

API ヘルプ

Alice は、Verify の API を利用して、ユーザー管理と認証などの ID 関連機能をアプリケーションに統合できます。Verify の API のヘルプには、必要な権限付与、パラメーター、およびレスポンス・メッセージの候補など、実装のためのガイダンスが記載されています。また、ヘルプ文書には、各 API 呼び出しの実装例も掲載されています。

次は：
カスタム・アプリケーションの
テンプレートの追加

The screenshot shows the IBM Security Verify API documentation for the 'Access Policy Management' endpoint. It includes a list of operations (GET, POST, DELETE, GET) with their respective URLs and descriptions. Below the operations, there are sections for 'Implementation Notes', 'Entitlements required', 'Response Class (Status 200)', and 'Parameters'. A JSON example response is also provided.

Access Policy Management

- GET /v1.0/policyvault/{policytag} Retrieve list of policies.
- POST /v1.0/policyvault/{policytag} Create a custom policy for tenant.
- DELETE /v1.0/policyvault/{policytag}/{id} Delete custom policy of tenant with specified id.
- GET /v1.0/policyvault/{policytag}/{id} Retrieve the details of a particular policy specified with id.

Implementation Notes

The REST interface to retrieve the policy for a specified ID. The **policytag** parameter needs to be specified. For access policy the value is "accesspolicy".

Entitlements required: readAccessPolicies (Read Access Policies)
OR
Entitlements required: manageAccessPolicies (Manage Access Policies)

Response Class (Status 200)

Success. The details policy was retrieved.

Model Example Value

```
{
  "predefined": false,
  "name": "Authentication policy",
  "format": "json",
  "rules": [
    {
      "conditions": "{ 'devicePlatform': ['MACOS', 'WINDOWS', 'OTHER_DESKTOP'] }",
      "name": "Platform Policy",
      "actions": "{ 'allowAccess': true }"
    }
  ]
}
```

Response Content Type: application/json

Parameter	Value	Description	Parameter Type	Data Type
policytag	accesspolicy (default)	Allowed policy tags: accesspolicy	path	string
id	[required]	The policy identifier.	path	long



従業員



ビジネス管理職



IT 管理者



開発者



開発者向け
リソース



カスタム・
アプリケーションの
構築



API の構成



戻る

次へ

開発者 : 1 / 4

カスタム・アプリケーションの構築

カスタム・アプリケーションのテンプレートの追加

Alice は、自分のカスタム・アプリケーションを、組織の他の SaaS とオンプレミス・アプリケーションとともに Verify の統合型シングル・サインオンに統合できます。まず、Alice はカスタム・アプリケーション・テンプレートを追加して、新規の SAML または OpenIDConnect アプリケーションを統合できます。

次は :
サインオン設定の構成



従業員



ビジネス管理職



IT 管理者



開発者



開発者向け
リソース



カスタム・
アプリケーション
の構築



API の構成



戻る

次へ

開発者 : 2 / 4

カスタム・アプリケーションの構築

サインオン設定の構成

アプリケーションのテンプレートでは、アプリケーションを統合するための段階的な指示が提供されます。

次は：
プロビジョニングの構成

Add Application

Custom Application

General | **Sign-on** | Account lifecycle

Sign-on method* SAML2.0

Provider ID* saml-provider-id
Unique identifier of the service provider. See the service provider documentation to get this value.

Use unique ID

Assertion consumer service URL (HTTP-POST)* https://acs.application.com/samlpost
[Add another URL](#)
The service provider endpoint that receives the SAML assertion. See the service provider documentation to get this value.

Use identity provider initiated single sign-on

Target URL
User is redirected to this page after single sign-on.

Service provider SSO URL
The endpoint that initiates the authentication request.

Signature options
Use digital signatures to establish trust between IBM Security Verify and the service provider.

Sign authentication response

Signature algorithm*

Third party SaaS application SAML2.0 single sign-on (SSO) configuration

Prerequisites

- Create an identity provider user that matches the login ID of your application.
- If third-party application expects attributes in the SAML assertion, configure the identity provider to pass those attributes in the SAML assertion.

Configure Third party SaaS application as the service provider (SP)
This procedure is generic and is applicable to any third-party SaaS application service provider. The details might vary depending on the application.

1. Log in to the third-party application administration console with your administrator user account.
2. Specify the following identity provider ID and URLs.
 - Provider ID**
`https://customer.verify.ibm.com/saml/sp/saml20ip/saml20`
 - If the **Use unique ID** check box is selected, use the following value:
`https://customer.verify.ibm.com/saml/sp/saml20ip/saml20/cc7fcc85562e4tc3`
 - Login URL**
`https://customer.verify.ibm.com/saml/sp/saml20ip/saml20/login`

Cancel Save



従業員



ビジネス管理職



IT 管理者



開発者



開発者向け
リソース



カスタム・
アプリケーション
の構築



API の構成



戻る

次へ

開発者 : 3 / 4

カスタム・アプリケーションの構築

プロビジョニングの構成

また、SCIM でアプリケーションの自動プロビジョニングとプロビジョニング解除を有効にすることもできます。

次は：
バグのトラブルシューティング

The screenshot shows the 'Add Application' configuration page in IBM Security Verify. The main heading is 'Custom Application'. The 'Account lifecycle' tab is active, showing settings for provisioning and deprovisioning accounts. Key sections include:

- Policies:** Options for 'Provision accounts' and 'Deprovision accounts', both set to 'Automatic'.
- Grace period (days)*:** Set to 30.
- Deprovision action:** Set to 'Delete account'.
- API authentication:** Fields for 'SCIM base URL*' (https://hr.customer.com/scim) and 'Bearer token*'. A 'Test connection' button is present.
- Third party SaaS application account lifecycle configuration:** A list of instructions for configuring the application for Bearer Token authentication.

At the bottom right of the configuration area, there are 'Cancel' and 'Save' buttons.



従業員

ビジネス管理職

IT 管理者

開発者

開発者向け
リソース

カスタム・
アプリケーション
の構築

API の構成



戻る

次へ

開発者: 4 / 4

カスタム・アプリケーションの構築

バグのトラブルシューティング

Alice は、アプリケーションのパフォーマンスを監視し、認証事象の詳細を調べて、バグのトラブルシューティングができます。

次は:
API クライアントの追加

The screenshot displays the IBM Security Verify console. On the left, the 'Application usage' report shows a line graph for 'Successful logins' with a peak of 8 on 04/27/2020. Below the graph is a table of login events:

Application	User Name	Realm	Location	Time	Status
Box	scott	cloudIdentityReal	Texas, United States	3:52:44 PM CDT	Success
Atlassian	alice	cloudIdentityReal	Texas, United States	3:33:34 PM CDT	Success
Atlassian	alice	cloudIdentityReal	Texas, United States	3:33:34 PM CDT	Success
Box	jessica@banedox.com	cloudIdentityReal	Texas, United States	3:33:34 PM CDT	Success

In the center, a 'SAML assertion' window is open, displaying XML code. The code includes details such as Issuer, Subject (NameID, SubjectConfirmation), Conditions (AudienceRestriction), AuthnStatement (AuthnContext, SessionIndex), and AttributeStatement (groups).

On the right, a 'SAML assertion' details panel shows 'Attributes sent' for the user 'scott@banedox.com', including roles like 'allUsers', 'admin', 'application owners', 'Legal', 'System admin', and 'developer'.



戻る

次へ

開発者 : 1 / 2

API の構成

API クライアントの追加

Alice はさまざまな API クライアントの中から選択して、自分のアプリケーションに統合できます。

次は:
委任管理

The screenshot shows the IBM Security Verify Configuration page. A modal dialog titled "Add API Client" is open. The dialog has the following sections:

- Name***: A text input field containing "Postman collection".
- Enabled**: A checked checkbox.
- Credentials**: Fields for Client ID and Client secret, both containing placeholder text.
- Custom scopes**: A checkbox for "Restrict custom scopes" which is unchecked.
- Access**: A section titled "Select the APIs that you want to grant access:" with a "Select All" toggle set to "Off". Below this are checkboxes for "Authenticate any user" (unchecked) and "Enable external agent runtime functions" (checked).
- Buttons**: "Cancel" and "Save" buttons at the bottom.

In the background, the "Configuration" page is visible, showing a table of API clients with columns for Name and Client ID. The table lists several clients like AgentConfig, All_Allowed_Access, ISAM API, Access session token, Registration, and Self-Service.



従業員



ビジネス管理職



IT 管理者



開発者



開発者向け
リソース



カスタム・
アプリケーション
の構築



API の構成



戻る

次へ

開発者 : 2 / 2

API の構成

委任管理

また、アクセス・トークンに付与された特定の API の権限付与を呼び出す権限をアプリケーションに付与することも可能です。

[IBM Security Verify の詳細はこちら](#)



The screenshot shows the 'Applications / Details' page for a 'Custom Application' (Developer App). The 'API access' tab is active, displaying a list of permissions. A 'Select All' toggle is currently 'Off'. The permissions list includes:

- Configure API access
- Access developer portal
- Access the admin console
- Authenticate any user
- Authenticate yourself
- Generate OTP
- Manage access certifications
- Manage access policies
- Manage access request
- Manage access request work flows
- Manage API clients
- Manage application entitlements
- Manage application lifecycle
- Manage attribute sources
- Manage authenticator configuration
- Manage authenticator registrations for all users
- Manage certificates
- Manage external agents
- Manage federations
- Manage identity sources
- Manage my activities approve or reject access request
- Manage OIDC and OAuth consents

Buttons for 'Delete', 'Cancel', and 'Save' are visible at the bottom of the configuration area.



従業員



ビジネス管理職



IT 管理者



開発者



開発者向け
リソース



カスタム・
アプリケーション
の構築



API の構成

© Copyright IBM Corporation 2021

日本アイ・ピー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町 19-21

アメリカ合衆国にて制作
2021年2月発行

IBM、IBM ロゴ、および ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、ibm.com/legal/copytrade.shtml で「著作権および商標情報」をご覧ください。

本資料は最初の発行日時点における最新情報を記載しており、予告なしに変更される場合があります。すべての製品が、IBM が営業を行っているすべての国において利用可能なものではありません。記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

本書に掲載されている情報は現状のまま提供され、第三者の権利の侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。

IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。お客様は自己の責任で関連法規を順守しなければならないものとします。IBM は法律上の助言を提供することはいたしませんし、また、IBM のサービスまたは製品が、お客様においていかなる法を遵守していることの裏付けとなることを表明し、保証するものでもありません。IBM の将来の方向性および指針に関する記述は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。

00000000USEN